LIEFF CABRASER HEIMANN & BERNSTEIN LLP
Elizabeth J. Cabraser (SBN 83151)
ecabraser@lchb.com
Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa A. Gardner (SBN 289096)
mgardner@lchb.com
Jallé Dafa (SBN 290637)
jdafa@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000

ROBBINS GELLER RUDMAN & DOWD LLP
Dorothy P. Antullis
Stuart A. Davidson
Lindsey H. Taylor
Nicolle B. Brito (333130)
Alexander C. Cohen
225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
dantullis@rgrdlaw.com
sdavidson@rgrdlaw.com
ltaylor@rgrdlaw.com
nbrito@rgrdlaw.com
acohen@rgrdlaw.com

Attorneys for Richard Roe, John Q. Public, and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

RICHARD ROE and JOHN Q. PUBLIC, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, vs. 23ANDME, INC., Defendant.	Case No. 3:24-cv-2319 CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Richard Roe ("Plaintiff Roe") and John Q. Public ("Plaintiff Public" and, collectively with Plaintiff Roe, "Plaintiffs"), individually and on behalf of all those similarly situated ("Class" or "Class members"), bring this Class Action Complaint ("Complaint") against Defendant 23andMe, Inc. ("23andMe," the "Company," or "Defendant") and allege upon personal knowledge as to their own actions and investigation of counsel, and upon information and belief as to all other matters, as follows:

1. Plaintiffs and Class members bring this action because their personally identifying information ("PII"), genetic information, and ancestry information (collectively, "Personal Information") was exfiltrated from Defendant's systems in a data breach discovered in or about August 2023 (the "Data Breach").

2. Hackers specifically targeted Plaintiffs' and Class members' genetic and ancestral information – which they provided in confidence to 23andMe – and posted it for sale on the dark web because of their Chinese and Ashkenazi Jewish genetic and ancestral information. Unlike many other data breaches, the hackers do not appear solely motivated to make money, but rather to target two at-risk populations. The danger to the Class is particularly acute given the antisemitism and anti-Asian ideology these groups face.

3. 23andMe's negligence, including leaving a fixable loophole allowing hackers access into its systems, were the direct cause of the Data Breach.

4. 23andMe's negligence is exacerbated by its failure to provide sufficient and timely notice to Class members, in particular those of Chinese and Ashkenazi Jewish descent, that their Personal Information is now available on the dark web to individuals who intend to threaten and harm them – and family members – as a result of their heritage and ancestry.

5. On October 6, 2023, Defendant first posted a notice in a blogpost on its website informing customers of the Data Breach. Specifically, Defendant stated that it had recently learned of suspicious activity in its database and in particular in its "DNA Relatives" feature and that information from its DNA Relatives feature had been "compiled" without the account users' authorization. It further stated that "threat actors" were able to gain access to certain accounts,

such as those where the user employed a recycled log in or a log in that had been hacked in another data breach. Defendant disclosed that it was investigating the Data Breach.

6. Notably, this initial notice was silent as to the hacker's motivations and that it had targeted profiles of descendants of Chinese and Ashkenazi Jewish customers, preventing Class members from taking immediate action.

7. In fact, as Defendant knew or should have known, the hackers had already posted an initial data sample of such information on the platform BreachForums.

8. Specifically, in an October 1, 2023 post, the hackers offered "the most valuable data you'll ever see" from 23andMe. They claimed to have one million data points exclusively about Ashkenazi Jews.[1] The BreachForums post indicated that they also had the Personal Information of hundreds of thousands of users of Chinese descent.

9. Moreover, the hackers had already begun selling what they claimed were 23andMe profiles for between $1 and $10 per account, depending upon the number of profiles being purchased.[2] 23andMe subsequently confirmed the legitimacy of the data.

10. On October 9, 2023, 23andMe provided an updated notice and once again did not provide critical information. Instead, it merely stated that its investigation was continuing, it had engaged third-party forensic experts, and it was working with federal law enforcement officials. It encouraged users to take precautions including resetting their passwords and using multi-factor authentication, but of course hackers had already exfiltrated Plaintiffs' and Class members' Personal Information.

11. About this time, Defendant sent another notice to impacted customers through an email that indicated the types of information hackers exfiltrated, including: (a) the customer's ancestry reports and matching deoxyribonucleic acid ("DNA") segments showing their genetic

[1] Lilly Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023), https://www.wired.com/story/23andme-credential-stuffing-data-stolen/; *23andMe Cyberbreach Exposes DNA Data, Potential Family Ties*, Dark Reading (Oct. 6, 2023), https://www.darkreading.com/attacks-breaches/23andMe-cyberbreach-exposed-dna-data-family-ties.

[2] *Id.*

ancestry, *i.e.* the percentage of their DNA that is attributable to their Chinese, Ashkenazi Jewish, or other heritage; (b) their relatives' DNA display names; (c) the predicted relationship and percentage of DNA shared with their relative matches; (d) birth location and profile picture; (e) birth year; and (f) a link to their family tree. This is the Personal Information that users provide 23andMe as part of their DNA Relatives profile.

12. On October 20, 2023, Defendant again updated its notice, and, for a fourth time, failed to provide information about the hackers' motivations and actions that were critical to Plaintiffs and Class members. Instead, 23andMe stated that it had disabled some of the features within the DNA Relatives tools as an additional precautionary measure to protect the privacy of its customers.

13. On the same day, a hacker, going by the alias "Golem," "dumped" the Personal Information of 23andMe's Ashkenazi Jewish customers on the dark web, apparently in retaliation for the Israel-Hamas war.

14. Although Defendant's public statements lay the blame for the Data Breach on its customers' reusing passwords that were previously hacked, technology experts have indicated that the Data Breach was due to a loophole in the Company's web design. As one commentator noted, a researcher revealed that 23andMe had a significant loophole in its website design, allowing anyone to view a user's profile by entering a profile ID into the URL.[3] The commentator stated, "This is a glaring oversight for a company dealing with such sensitive data."[4]

15. The Data Breach of genetic material of Class members, including descendants of Ashkenazi Jews, is especially dangerous and compromises the security of Class members. Indeed,

[3] Tom Donovan, *23andMe Data Breach*, The Final Hop (Oct. 6, 2023), https://www.thefinalhop.com/23andMe-data-breach.

[4] *Id.*

the *Wall Street Journal* posted an editorial entitled, "The Global War on the Jews," noting that antisemitism is surging on a worldwide basis.[5]

16. Due to the Data Breach, Class members face a significantly increased and ongoing risk of potential hate crimes and discrimination due to information about their genetic ancestry becoming public.

17. The fact that the hacker uses the alias "Golem" – a clay figure in Hebrew folklore that is brought to life in times of peril to the Jewish people – indicates that the Data Breach may have been politically and/or racially motivated and was seemingly specifically deemed to target those of Jewish descent.[6]

18. For example, "Golem's" post advertising the exfiltrated Personal Information described it as being "Great Britain-Originated" data that contained "samples from hundreds of families, including . . . . [the] Rothschilds," a well-known Jewish banking family that is the subject of anti-Semitic conspiracy theories.

19. Plaintiffs and Class members have suffered and will continue to suffer injury as a direct and proximate result of 23andMe's negligent, reckless, or intentional conduct, including:

(a) the decrease in their physical security and the out-of-pocket costs to increase security measures and ensure that they are protected;

(b) increased concern that further Personal Information increased emotional distress that they can now be identified as of Chinese or Jewish, and thus subjected to anti-Semitic and anti-Asian acts;

(c) out-of-pocket losses associated with preventing, detecting and remediating identify theft or other unauthorized uses of their Personal Information;

(d) the lost or diminished value of their Personal Information;

---

[5] *The Global War on the Jews*, Wall St. J. (Oct. 30, 2023), https://www.wsj.com/articles/israel-hamas-jews-pogroms-russia-u-s-europe-germany-anti-semitism-1a74109c?mod=Searchresults_pos1&page=1.

[6] Scott Ikeda, *Second Leak From 23andMe Data Breach Includes 4 Million More Genetic Profiles*, CPO Magazine (Oct. 25, 2023), https://www.cpomagazine.com/cyber-security/second-leak-from-23andMe-data-breach-includes-4-million-more-genetic-profiles/.

(e) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach;

(f) the loss of the benefit of their bargain for Defendant's services,

(g) the invasion of their privacy; and

(h) the theft of their Personal Information and loss of privacy rights.

20. As a direct and proximate result of 23andMe's breach of confidence and failure to protect their Personal Information, Plaintiffs and Class members have been injured by facing ongoing, imminent, impending threats of hate and identity theft crimes, fraud, scams, and other misuses of their Personal Information; ongoing monetary loss and economic harm; loss of value of privacy and confidentiality of the stolen Personal Information; illegal sales of the compromised Personal Information; loss of the benefit of their bargain, mitigation expenses and other injuries. Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

I. Jurisdiction and Venue

21. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. §1332(d) because: (a) there are 100 or more putative Class members; (b) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest and costs; and (c) there is minimal diversity because Plaintiffs and Defendant are citizens of different states.

22. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

23. This Court has personal jurisdiction over Defendant because the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District. Defendant's principal place of business is also located in this District.

24. Venue in this District is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to the claims occurred in the Northern District of California.

II. INTRADISTRICT ASSIGNMENT

25. Pursuant to Civil L.R. 3-2(c), assignment to this Division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this District. Defendant markets its products throughout the United States, including in San Francisco county.[7]

III. Parties

26. Plaintiff Roe is an individual who is a citizen of the State of Florida and is an Ashkenazi Jew.

27. Plaintiff Roe was a user of Defendant's services and received an email notice ("Notice") from Defendant on December 29, 2023, informing him that he was identified as having been impacted by the Data Breach.

28. Plaintiff Public is an individual who is a citizen of the State of New Jersey and is an Ashkenazi Jew.

29. Plaintiff Public was a user of Defendant's services and received a Notice from Defendant in October, 2023, informing him that he was identified as having been impacted by the Data Breach.

30. Plaintiffs suffered actual injury and are continuing to suffer actual and imminent danger as a consequence of this seemingly anti-Semitic and politically motivated Data Breach, because: (a) their identity as Ashkenazi Jews was made public, thereby placing them and others in the Class in a particularly dangerous and precarious situation; and (b) their Personal Information was compromised causing: (i) damage to and diminution in the value of their Personal Information that 23andMe obtained from Plaintiffs; (ii) loss of the benefit of the bargain for Defendant's services; (iii) violation of Plaintiffs' privacy rights; and (iv) present and increased risk arising from the hate crimes, identity theft, and fraud.

31. As a result of the Data Breach, Plaintiffs have spent and, going forward, anticipate spending considerable time and money on an ongoing basis to try to mitigate and address the harms

[7] Further, the Judicial Panel on Multi-District Litigation transferred several related cases to Judge Chen in the San Francisco division and Plaintiffs intend to file a notice of related cases pursuant to Civil L.R. 3-12 herewith.

caused by the Data Breach. As a result of the Data Breach, Plaintiffs are and will continue to be at increased risk of hate crimes, and identity theft and fraud for years to come.

32. Defendant 23andMe, Inc. is a Delaware corporation registered with the California Secretary of State, with its principal place of business and headquarters located at 223 North Mathilda Venue, Sunnyvale, California 94086.

IV. Background

A. 23andMe Promised to Protect Customers' Privacy

33. 23andMe is a home-based genetics testing company that commenced business around 2006. It operates through either a website or mobile application, in which customers create an account and then purchase a DNA testing kit.

34. Customers sign up for a particular package, such as the basic ancestry service, the health and ancestry service or the full membership, which range in price from $119 to $298. They then receive a genetic testing kit, through which they take their own saliva samples, place them in a tube, and mail the sample back to the testing company.

35. From there, a laboratory isolates the DNA, runs genetic tests and interprets the results providing customers with both information about their genetic background and potential health risks based upon their genetic background, such as predisposition and carrier status for certain cancers, Alzheimer's disease, diabetes, cystic fibrosis, sickle cell anemia, and other conditions, depending upon the package they choose.

36. 23andMe's Ancestry Services has about 12 million members. Customers with a basic package receive an analysis of their ancestry percentages, informing them of the percentages of their ancestry, and where in the world their DNA is from, out of over 2,750 regions. They also receive an ancestry report, giving the customer a granular view of their ancestry backgrounds, including curated content on the history, food, and popular travel destinations connected to their DNA.

37. If a customer purchases the optional DNA Relatives feature, 23andMe will also take the customer's DNA and match it to their relatives' DNA in the 23andMe database, enabling the customer to connect with those who have some percentage or overlap of the same DNA.

Through the DNA Relatives feature, customers can uncover unknown relatives and build a family tree.

38. Ancestral History traces a customer's ancestry timeline, informing them of the number of generations back that their family fell into certain categories or the groups or regions from which the customer is descended, with one example being Ashkenazi Jewish.

39. Given the sensitivity of the information provided by customers, 23andMe's Privacy Statement specifically represents and assures customers that their Personal Information will be protected.

40. On its website, 23andMe specifically represents to its customers that "**Your privacy comes first**," and states:

> When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected.

41. It reiterates this representation in its Privacy Statement under "Security Measures," explaining:

> We implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information. Our team regularly reviews and improves security practices to help ensure the integrity of our systems and your Personal Information.

42. In the section entitled "How is my Personal Information Protected?" Defendant assures customers that it takes all necessary steps to prevent unauthorized access to Personal Information, against stating:

> 23andMe takes seriously the trust you place in us. To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of information, 23andMe uses a range of physical, technical, and administrative measures to safeguard your Personal Information, in accordance with current technological and industry standards. In particular, all connections to and from our website are encrypted using Secure Socket Lays (SSL) technology.

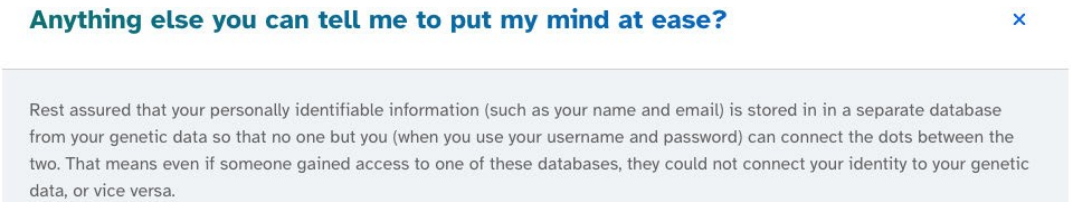
43. 23andMe further assures customers that its data security protocols "exceed industry data protection standards," that it "encrypt[s] all sensitive information," and also "conduct[s] regular assessments to identify security vulnerabilities and threats."

44. 23andMe also expressly tells users that it understands the threat of hackers and the severity of the consequences of a potential data breach, as shown in Figure 1 below, which is a screenshot from its website.

(Figure 1)

45. On its blog, the company goes further, stating that "23andMe access combines token-based, multi-factor authentication and strict least-privileged authorization controls."

46. Defendant also tells potential customers that they should not be concerned about their private genetic information being exposed because the company untethers its customers' identities from the genetic data stored on its servers. In response to a hypothetical question, "Anything else you can tell me to put my mind at ease," Defendant promises that PII is segregated from genetic data, so that "no one but you . . . can connect the dots between the two," as shown in Figure 2 below, which is a screenshot from its website.



(Figure 2)

47. In other words, 23andMe assures customers that even if breached, their genetic data will remain protected and unconnected to their identities.

48. These statements are meant to assure customers that their genetic data will not be at risk of disclosure and that they have full control over how it is shared. This message is bolstered by representations from 23andMe that "you are in control of your DNA and your data" and "we give you full control to decide how your information is used and with whom it is shared."

49. 23andMe's customers chose to purchase the company's services with the expectation that it would comply with its promises to keep such information confidential and secure from third parties.

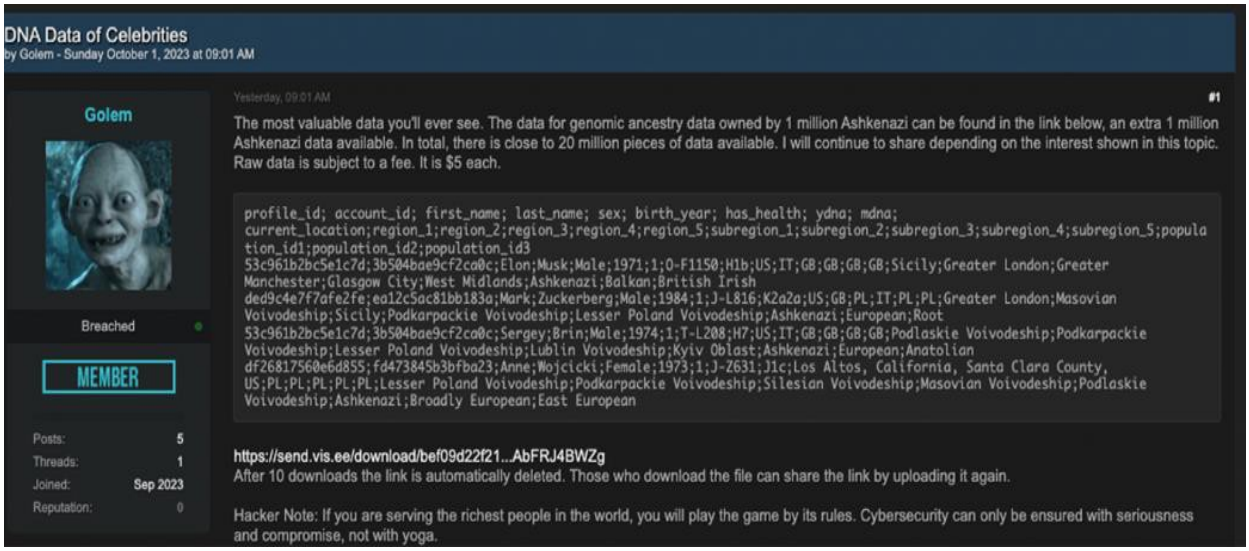
50. While 23andMe assured customers of the numerous steps it takes to protect their privacy, the Data Breach has shown these representations to be false, including 23andMe's specific promises that it anonymizes the genetic information stored on its servers, protects Personal Information using protocols that "exceed" industry standards, and actively monitors for suspicious activity.

B. Despite its Data Security Promises, 23andMe's Customers' Private Genetic Information was Stolen and Used to Target Vulnerable Groups.

51. Hackers use the "dark web" to buy, sell, and otherwise release stolen data. The dark web is accessible via The Onion Router ("TOR"), which redirects traffic through thousands of relays in order to anonymize the user's internet activity and browsing. While using TOR, the websites that are visited only log the IP address of the last TOR relay, as opposed to the user's actual IP address. TOR mainly consists of Onion sites that are similar to normal websites but end with an address of ".onion." These sites can only be visited through a TOR interface. Just like the surface web, the dark web has various search engines that can be used to find content.

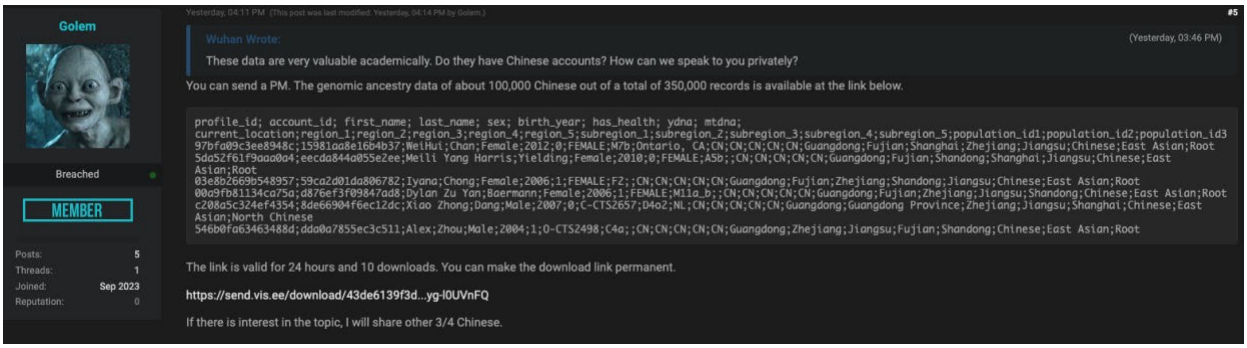
52. Cybercrime forums such as BreachForums are utilized by users on the dark web to anonymously advertise and purchase stolen information, including stolen databases, leaks from ransomware or other malicious software, and compromised accounts and passwords.

53. On October 1, 2023, a hacker using the alias "Golem" leaked the 23andMe DNA and profile data of one million Ashkenazi Jews, including their full names, home addresses, and birth dates on BreachForums, calling it "[t]he most valuable data you'll ever see," as shown in Figure 3 below, a screenshot from BreachForums.



(Figure 3)

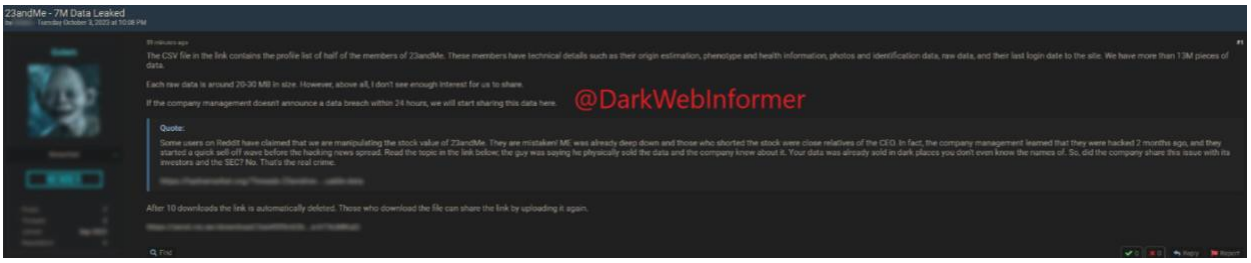
54. A few hours after leaking the Jewish 23andMe database, a user with the alias "Wuhan" replied and asked Golem if has "Chinese accounts," indicated that such data is "very valuable academically," and asked if they could "speak privately." Golem responded with a link to the DNA and profile data of 100,000 Chinese customers. Golem also stated that he has "a total of 350,000" DNA and profile records and that he would release them if there was interest, as shown in Figure 4 below, a screenshot from BreachForums.



(Figure 4)

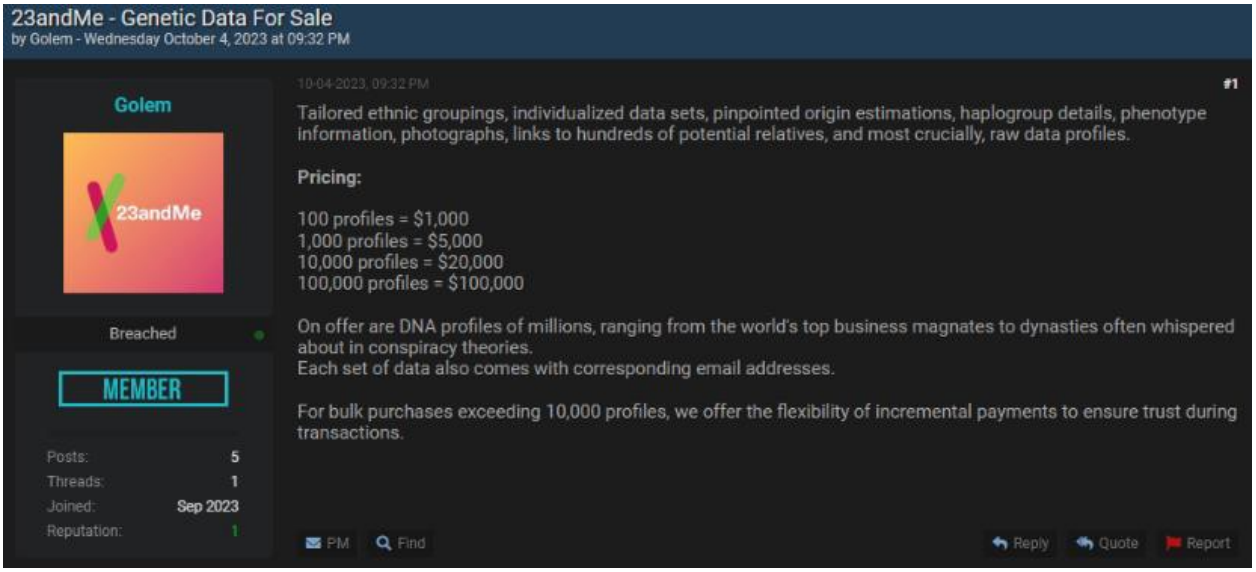
55. The next day, Golem leaked an even larger database of information including the DNA and profile data of seven million users. Golem shared a link to the stolen data, writing, "the CSV file in the link contains the profile list of half of the members of 23andMe . . . these members have technical details such as their origin estimation, phenotype and health information, photos and

identification data, raw data, and their last login date to the site," as shown in Figure 5 below, a screenshot from BreachForums taken by Dark Web Informer:



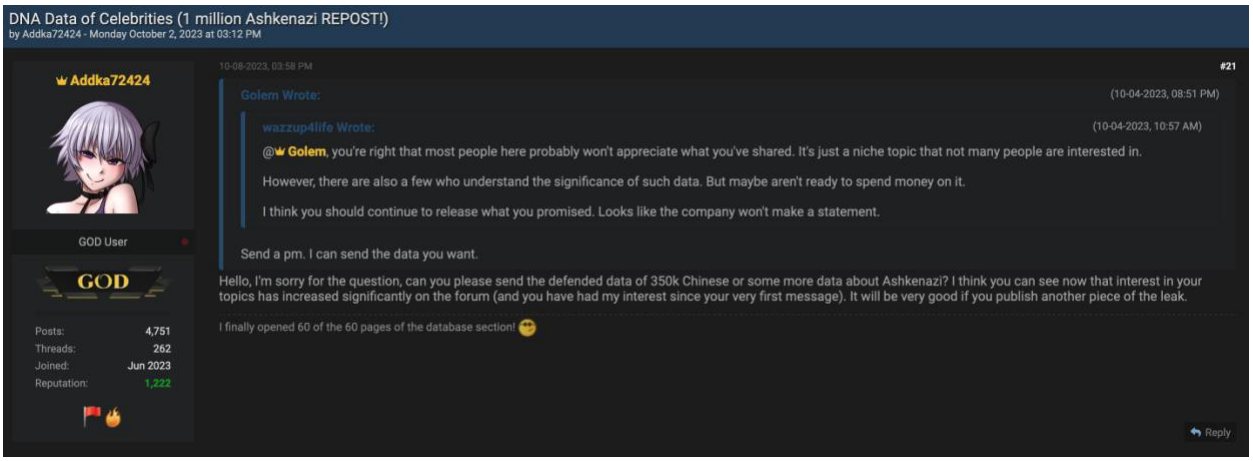
(Figure 5)

56. On October 3, 2023, Golem posted pricing for "[t]ailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to hundreds of potential relatives, and most crucially, raw data profiles," as shown in Figure 6 below, a screenshot from BreachForums.



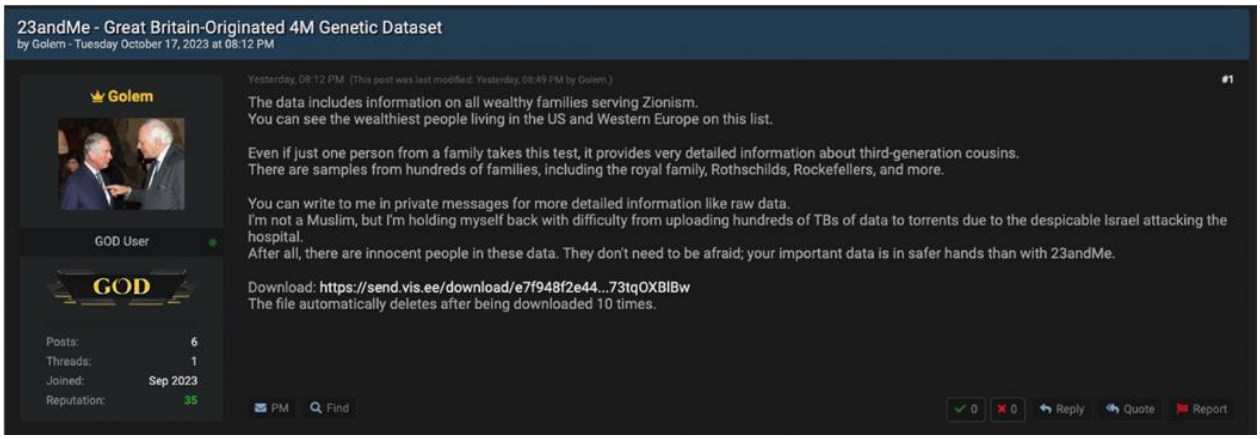
(Figure 6)

57. The Chinese and Jewish leaks were met with immediate and overwhelming interest from other BreachForums users. For example, on October 8, 2023, "Addka72424" replied to Golem, stating, "I think you can see now that interest in your topics has increased significantly on the forum (and you have had my interest since your very first message)" and asked, "can you please send the defended data of 350k Chinese or some more data about Ashkenazi?" as shown in Figure 7 below, a screenshot from BreachForums.



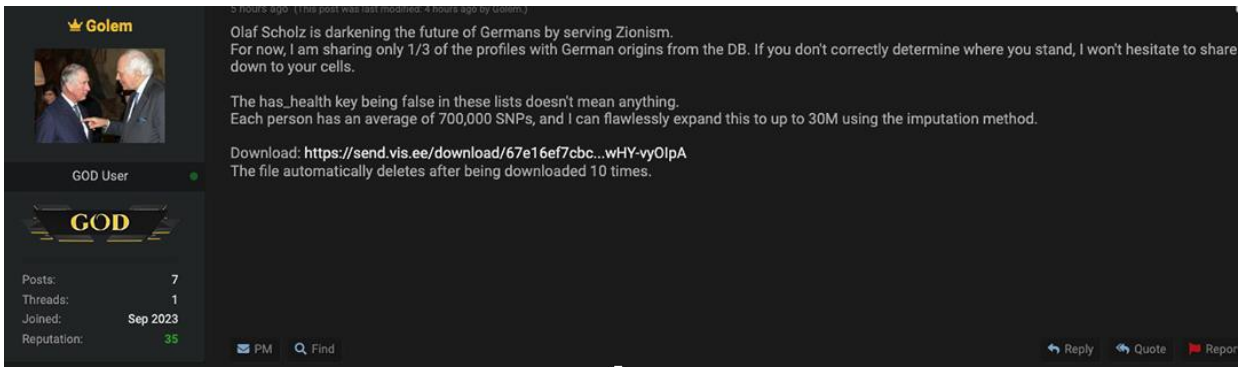
(Figure 7)

58. On October 17, 2023, Golem posted another thread titled "23andMe – Great Britain-Originated 4M Genetic Dataset," that expounded on his apparent anti-Semitic agenda and included data about "wealthy families serving Zionism" and stated, "I'm not a Muslim, but I'm holding myself back with difficulty from uploading hundreds of TBs [terabytes] of data to torrents due to the despicable Israel attacking the hospital," shown below in Figure 8, a screenshot from BreachForums.



(Figure 8)

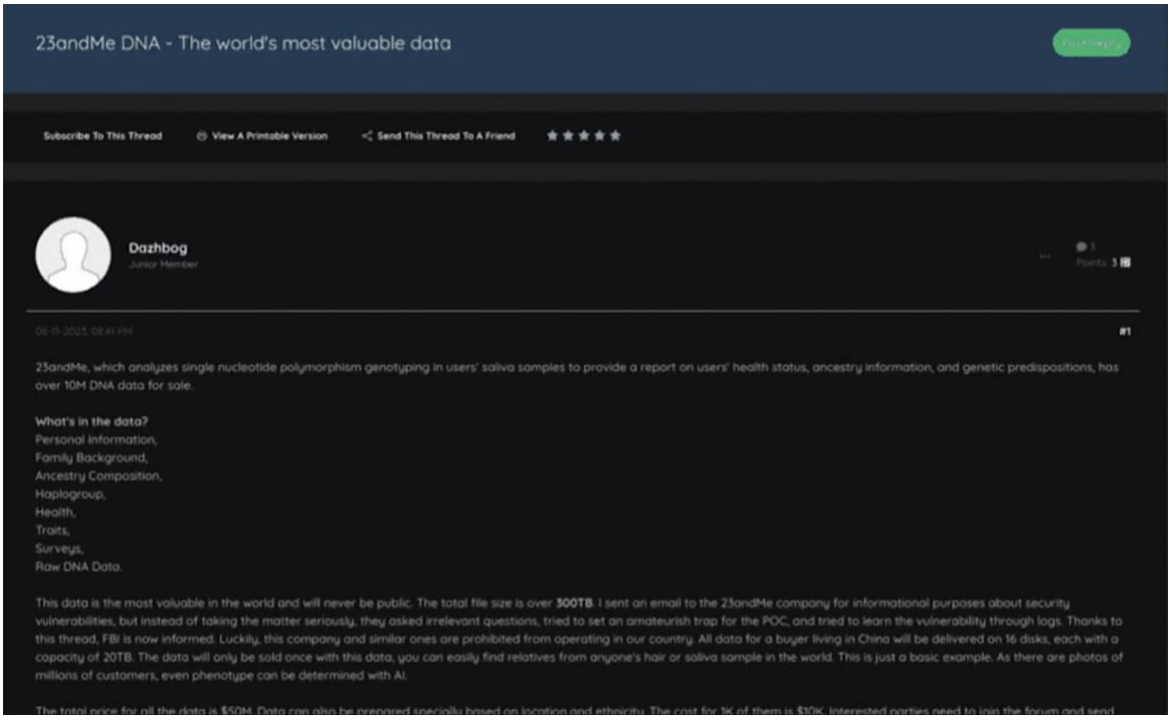
59. One day later – after German Chancellor Olaf Scholz expressed solidarity with Israel at a press conference in Tel Aviv with Israeli Prime Minister Benjamin Netanyahu – Golem posted another message stating that "Olaf Scholz is darkening the future of Germans by serving Zionism," and noting that he had profiles "with German origins" as shown in Figure 9 below, screenshot from BreachForums.



(Figure 9)

60. Reports show that there may have also been an additional and entirely separate breach of 23andMe's servers by a different threat actor several months before the Personal Information was posted to BreachForums on October 1, 2023.

61. On August 11, 2023, a person using the alias "Dazhbog" posted a message titled, "23andMe DNA – the world's most valuable data," on a hacker forum called Hydra Market offering to sell 300 terabytes of 23andMe data for $50 million and stating that "all data for a buyer living in China will be delivered on 16 disks, each with a capacity of 20 TB," as shown in Figure 10 below, a screenshot from Hydra Market:



(Figure 10)

62. On August 12, 2023, Dazhbog uploaded a sample of genetic data for one million 23andMe customers in the United States, noting that it possessed the DNA profiles of 10 million Americans. The hacker claimed to have contacted 23andMe at that time—a relatively common extortion practice—but "instead of taking the matter seriously, [the company] asked irrelevant questions."

63. At this time, Plaintiffs do not know if the Dazhbog leak contained authentic 23andMe customer information or if 23andMe was even aware of the posting, as it never publicly acknowledged the post or notified its customers about it. Plaintiffs are also unaware at this time as to whether the Dazhbog and Golem leaks are related in any way. These matters will be explored through discovery.

64. However, the fact that there is evidence of a potential additional breach of 23andMe's customers' genetic information that occurred two months earlier is nonetheless extremely concerning, especially given that Dazhbog provided specific instructions about how it would safely deliver this data to China.

65. The disclosure of the Chinese and Jewish customer lists threatens the safety and security of those customers and subjects them to harassment, vandalism, assault, intimidation, and discrimination.

66. Nevertheless, to this day, Defendant has failed to notify any of its Chinese or Ashkenazi Jewish customers that their DNA, genetic reports, and personal information has been leaked on BreachForums and shared with an untold number of hackers.

C. 23andMe Announces the Data Breach

67. On October 6, 2023, 23andMe first disclosed information about the Data Breach, ("October 6 Announcement"), stating:

> We recently learned that certain 23andMe customer profile information that he opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.
>
> After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is,

> usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked.
>
> We believe that the threat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service.

68. 23andMe then went on to falsely assure customers that it was committed to safety and security stating:

> Committed to Safety and Security
>
> 23andMe is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected. We are continuing to investigate to confirm these preliminary results. We do not have any indication at this time that there has been a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.
>
> At 23andMe we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate. Since 2019 we've offered and encouraged users to use multi-factor authentication (MFA), which provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords.

69. The October 6 Announcement failed to provide any details on the number of customers affected by the breach, and most importantly, failed to mention that the hacker leaked the DNA and profile information of seven million customers on the dark web or that the hacker disclosed specially curated lists of Chinese and Jewish customers. In fact, to this day, 23andMe has never told its customers about the BreachForums leak, even though its spokesperson has confirmed for multiple media outlets that the leak contained genuine data.

70. Instead of providing this critical information or explaining what steps were being taken to remedy its data security vulnerabilities, 23andMe's October 6 Announcement blamed its customers, telling them that the breach was the result of "threat actors [who] were able to access certain accounts in instances where users recycled login credentials—that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked." 23andMe also reassured that customer data is adequately protected on its system, reiterating that "At 23andMe, we take security seriously. We exceed industry data

protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected."

71. 23andMe recommended to customers that they change their passwords and take other protective actions.

72. 23andMe updated its online notice again on October 9 and October 20, 2023, each time noting that it was in the midst of an ongoing investigation, and urging customers to change their passwords and use multi-factor authentication. On November 6, 2023, 23andMe began requiring the use of two-step verification for customers to access their accounts.

73. On about October 10, 2023, 23andMe first sent out an email notice (the "October 10 Notice") to some customers whose Personal Information had been hacked.

74. In the October 10 Notice, 23andMe admitted that "certain profile information – which a customer creates and chooses to share with his genetic relatives in the DNA Relatives feature – was accessed from individual 23andMe.com accounts." The October 10 Notice further states that, this access was done "without the account users' authorization." 23andMe further explained that it was engaged in an ongoing investigation and that it believed that the threat actors had used passwords that had been subject to earlier hacks of other platforms.

75. Similar to its online notice, the October 10 Notice said nothing about the fact that the Data Breach was apparently politically and/or racially motivated and that Ashkenazi Jews and those of Chinese descent had been targeted and that their information was already being sold on the dark web.

76. 23andMe disseminated another notice a few days later, on about October 13, 2023 (the "October 13 Notice"). The October 13 Notice disclosed to customers that the their profile information had been part of the Data Breach, including and most importantly, the analysis of their ancestry and ancestry report and matching DNA segments, their relatives' DNA and the percentage of DNA shared with their matches, their name and state of residence, their DNA Relatives display names, their birth year, and how recently they had logged in – in other words, all the information

that someone seeking to perpetrate a hate crime against an individual would need to identify them as Chinese or Jewish, and track them down.

77. On December 1, 2023, Defendant updated its October 6 Announcement to report that "23andMe has completed its investigation, assisted by third-party forensic experts," and is finally "in the process of notifying affected customers." In other words, 23andMe waited a full two months before it informed seven million customers that they were directly impacted by the data breach, and even then, the section titled '"How does this impact you?" was so vague and confusing that it raised more questions than it answered, as shown in Figure 11 below, a screenshot of that section from 23andMe's December 1, 2023 email notice:

> **How does this impact you?**
> After further review, we have identified your DNA Relatives profile as one that was impacted in this incident. Specifically, there was unauthorized access to one or more 23andMe accounts that were connected to you through DNA Relatives. As a result, the DNA Relatives profile information you provided in this feature was exposed to the threat actor. You can see a full list of the types of information that you may have included in your profile here. You can view what information is currently included in your DNA Relatives profile and make changes here.

(Figure 11)

78. Amazingly, Defendant again concealed the BreachForums leak and again failed to notify customers with Chinese or Ashkenazi Jewish ancestry that they were specifically targeted by hackers.

79. On December 5, 2023, Defendant provided its most recent update to the October 6 Announcement:

> As our investigation comes to a close, we wanted to share the details of what took place and our findings. In early October, we learned that a threat actor accessed a select number of individual 23andMe.com accounts through a process called credential stuffing. That is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously compromised or otherwise available. We do not have any indication that there was a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.
>
> The threat actor used the compromised accounts to access information shared with

these accounts. Specifically, DNA Relatives profiles connected to these compromised accounts, which consist of information that a customer chooses to make available to their genetic relatives when they opt in to participate in 23andMe's DNA Relatives feature. A DNA Relatives profile includes information such as display name, predicted relationships, and percentage of DNA shared with matches. You can find a full list of the types of information included in a DNA Relatives profile here.

Additionally, through the compromised accounts, the threat actor accessed a feature called Family Tree, which includes a limited subset of DNA Relatives profile information. The Family Tree feature does not include ancestry information such as the percentage of DNA shared with genetic matches or ancestry reports.

Additional Details

- The threat actor was able to access less than 0.1%, or roughly 14,000 user accounts, of the existing 14 million 23andMe customers through credential stuffing.
- The threat actor used the compromised credential stuffed accounts to access the information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million), each of which were connected to the compromised accounts.

Since detecting the incident, we emailed all customers to notify them of the investigation and are continuing to notify impacted customers, based on applicable laws. We also required every 23andMe customer to reset their password. In addition, 23andMe now requires all new and existing customers to login using two-step verification. Protecting our customers' data privacy and security remains a top priority for 23andMe, and we will continue to invest in protecting our systems and data.

80. 23andMe's most recent public announcement fell woefully short of providing any information about the Data Breach and again failed to warn victims that their Personal information had already been leaked on BreachForums. By failing to disclose this critical information, 23andMe lied to its customers about the scope and severity of the breach.

81. Further, despite having actual knowledge that the hacker curated and leaked lists of Chinese and Jewish customers on the dark web, a 23andMe spokesperson told the *New York Times* on December 4, 2023, that "we have not learned of any reports of inappropriate use of the data after the leak."[8] Likewise, 23andMe's attorney, Ian Ballon, went even further in a December 11, 2023 letter to attorneys representing certain 23andMe customers, stating, "the information that was

[8] Rebecca Carballo, *Data Breach at 23andMe Affects 6.9 Million Profiles, Company Says*, NEW YORK TIMES (Dec. 4, 2023), https://www.nytimes.com/2023/12/04/us/23andme-hack- data.html.

potentially accessed cannot be used for any harm."[9] These were false statements that were intended to mislead 23andMe's customers and investors.

D. The Data Breach Was a Foreseeable Risk of Which Defendant Was on Notice

82. It is well known that PII is a valuable commodity and a frequent, intentional target of cyber criminals and hackers. Companies that collect such information, including Defendant, are well aware of the risk of being targeted by hackers and cybercriminals.

83. In 2021, for instance, there was a record 1,862 data breaches surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[10]

84. Genetic or ancestry material is also extremely valuable, especially as hackers can sell that material to insurance companies, sell it on the "low down" or in this case, use to threaten members of particular racial or religious groups, as disclosed by their genetic testing.[11]

85. Several genetic testing entities have been the subject of well publicized hacks or data breaches, of which Defendant was or should have been aware, particularly given its previously mentioned representation that it "regularly reviews and improves security practices to help ensure the integrity of our systems and your Personal Information."

86. For example, several months ago, 1Health.io, another genetics testing company, was fined $75,000 by the Federal Trade Commission ("FTC") for failing to secure sensitive data. In 2021, the Ohio and Pennsylvania States Attorney General fined DNA Diagnostic Center, a DNA

---

[9] Letter from Ian C. Ballon, Attorney for 23andMe, to Hassan A. Zavareei (Dec. 11, 2023) available at https://www.documentcloud.org/documents/24252535-response-letter-to-tycko-zavareei-llp.

[10] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/.

[11] Angela Chen, *Why a DNA data breach is much worse than a credit card leak*, Center for Genetics and Society (June 6, 2018), https://www.geneticsandsociety.org/article/why-dna-data-breach-much-worse-credit-card-leak.

testing entity, $400,000 for a data breach that affected 2.1 million customers.[12] And in 2018, hackers breached the accounts of 92 million customers of MyHeritage, although the hackers never reached actual genetic data.[13]

87. Therefore, 23andMe was well aware that it could be subject to a hack, and that the genetic and ancestral information that it maintained was valuable and attractive to hackers, but yet it failed to take steps to close the loophole on its website that would have prevented the Data Breach.

88. Since that time, the data for Ashkenazi Jews has appeared on the dark web. An NBC Report on October 7, 2023, stated that *NBC News* had a list of 999,999 people who allegedly used 23andMe, which was being shared on the internet.

89. The database, which showed up on the dark web, included the first and last names of Jewish customers, their sex, and 23andMe's evaluation of where their ancestors came from. It was entitled, "Ashkenazi DNA Data of Celebrities," although most of the people in the database were not famous and, according to NBC News, appears to be sorted to have only included people with Ashkenazi heritage.[14]

E. 23andMe Is Under Investigation

90. Given the apparent political and anti-Semitic nature of the Data Breach, and threats from the hacker named Golem in the aftermath, 23andMe is now under Congressional and state investigation.

91. On October 20, 2023, Senator Bill Cassidy, the Ranking Member of the Senate Committee on Health, Education, Labor and Pensions, sent a letter to Ann Wojcicki, 23andMe's

[12] Apurva Venkat, *DNA Diagnostic Center fined $400,000 for 2021 data breach*, CSO (Feb. 21, 2023), https://www.csoonline.com/article/574597/dna-diagnostic-center-fined-400-000-for-2021-data-breach.html.

[13] Angela Chen, *supra* note 10.

[14] Kevin Collier, *23andMe user data targeting Ashkenazi Jews leaked online*, NBC News, Oct. 7, 2023, https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-leaked-online-rcna119324.

Chief Executive Officer (the "October 20 Letter") noting his concern regarding the Data Breach and requesting the production of certain information pertaining to it.[15]

92. In the October 20 Letter, Senator Cassidy stated that he was particularly concerned with the "unauthorized disclosure of 1.3 million customers' information being posted on the dark web, including one million customers identified as people of Ashkenazi Jewish descent and 300 thousand [sic] customers identified as people of Chinese heritage."[16]

93. Senator Cassidy further stated that the disclosed data included name, sex, birth year, location, photos, health information and genetic ancestry results, and that this information was shared online as a database entitled, "Ashkenazi DNA Data of Celebrities."[17] He noted the danger in which that disclosure placed those Ashkenazi Jews whose information had been disclosed, citing to one poster who claimed, "Crazy, this could be used by Nazis," which is particularly concerning given the "increasing rates of global antisemitism and anti-Asian hate, which can be leveraged to draw higher prices for the information and increase the threat from potential evildoers." He noted that the records were selling for between $1 and $10 each.[18]

94. The October 20 Letter further explained that the Data Breach could have implications far beyond that incident and gave the Company until November 3, 2023. to answer a number of pertinent questions including how only a few compromised user accounts could provide hackers with information for hundreds of personal accounts, and what the Company was doing to compensate affected users.

95. On about October 30, 2023, the Connecticut Attorney General, William Tong, sent Jacquie Cooke, 23andMe's General Counsel and Privacy Officer, a similar letter entitled, "Data

---

[15] *Ranking Member Cassidy Raises Concerns over 23andMe Data Leaks, Potential Targeting of Minority Groups*, U.S. Senate Committee on Health, Education Labor & Pensions (Oct. 20, 2023), https://www.help.senate.gov/ranking/newsroom/press/ranking-member-cassidy-raises-concerns-over-23andMe-data-leaks-potential-targeting-of-minority-groups.

[16] *Id.*

[17] *Id.*

[18] *Id.*

Breach" (the "October 30 AG Letter") pertaining to how the Data Breach affected Connecticut residents.[19]

96. In the October 30 AG Letter, Attorney General Tong also noted his concern that a hack targeting Jewish and Asian customers was particularly dangerous given the anti-Semitic and anti-Asian rhetoric and violence in recent years. *Id.* at 1. Attorney General Tong further stated that 23andMe was required to but had failed to comply with Connecticut's notice requirements and may well have violated the Connecticut Data Privacy Act.[20]

97. Attorney General Tong similarly posed a number of poignant questions to 23andMe, including whether the Company intended to comply with Connecticut's notice requirement and what kind of safeguards it had in place to prevent "credential stuffing" and requested responses by November 13, 2023.

F. Facts Pertinent to Plaintiff Roe and Plaintiff Public

98. Plaintiff Roe first registered with 23andMe in July 2018 in order to research his genealogical background and attempt to connect with family members.

99. At that time, Plaintiff Roe signed up for the 23andMe package and opted for the DNA Relatives Finder.

100. Plaintiff Roe proceeded to provide 23andMe with his saliva sample, believing that his genetic make-up and his ancestry would be protected by Defendant, given its representations respecting the security of information provided to it. He also provided detailed information about his known family members.

101. Thereafter, Plaintiff Roe received his ancestry analysis, disclosing that a significant percentage of his ancestry is Ashkenazi Jewish.

[19] Letter to Jacquie Cooke, General Counsel and Privacy Officer, 23andMe Inc. from William Tong, Attorney General, Office of the Attorney General Connecticut (Oct. 30, 2023), https://portal.ct.gov/-/media/AG/Press_Releases/2023/10-30-2023-William-Tong--23andMe-Inc-Inquiry-Letter-final-002.pdf.

[20] *Id.* at 2.

102. Ashkenazi Jews, for the most part, are descended from Central and Eastern European countries. About half of all Jewish people are Ashkenazi.

103. Plaintiff Roe also obtained a list of the names of his DNA Relatives, the percentage of DNA that he shares with each one, and his relationship to him, for example, a second cousin.

104. Thereafter, Plaintiff Roe continued to maintain his DNA Relatives Finder option, which was periodically updated.

105. In or around October 2023, Plaintiff Roe learned of the Data Breach through news reports and made the decision to close his 23andMe account.

106. On December 29, 2023, Plaintiff Roe received an email Notice from 23andMe disclosing that the Company had suffered an unauthorized intrusion and that records from his DNA Relatives feature, including his Family Tree profile, had been accessed by "a threat actor." 23andMe again touted that security and privacy are its highest priorities, and it routinely monitors and audits its systems.

107. Plaintiff Public first registered with 23andMe in 2021 in order to research his genealogical background and attempt to connect with family members.

108. At that time, Plaintiff Public signed up for the 23andMe package and opted for the DNA Relatives Finder.

109. Plaintiff Public proceeded to provide 23andMe with his saliva sample, believing that his genetic make-up and his ancestry would be protected by Defendant, given its representations respecting the security of information provided to it.

110. Thereafter, Plaintiff Public received his ancestry analysis, disclosing that a significant percentage of his ancestry is Ashkenazi Jewish.

111. Plaintiff Public also obtained a list of the names of his DNA Relatives, the percentage of DNA that he shares with each one, and his relationship to him, for example, a second cousin.

112. Thereafter, Plaintiff Public continued to maintain his DNA Relatives Finder option, which was periodically updated.

113. In or around October 2023, Plaintiff Public learned of the Data Breach through emails sent to him by 23andMe.

114. As both the October 20 Letter from Senator Cassidy and the October 30 Letter from Attorney General Tong indicated, the Data Breach and disclosure of genetic and ancestry information for those of Chinese and Ashkenazi Jewish descent is particularly dangerous.

G. 23andMe had a Duty to Plaintiffs and Class Members

115. At all relevant times, 23andMe had a legal and equitable duty to Plaintiffs and Class members to properly secure their Personal Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class members, and to ***promptly*** notify Plaintiffs and Class members when Defendant became aware that their Personal Information was compromised.

116. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between 23andMe and Plaintiffs and Class members. The special relationship arose because Plaintiffs and Class members entrusted 23andMe with their Personal Information when they were customers.

117. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class members.

118. Security standards commonly accepted among businesses that store Personal Information using the internet include:

(a) Maintain a firewall configuration;

(b) Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

(c) Monitoring for suspicious or irregular traffic to servers;

(d) Monitoring for suspicious credentials use to access servers;

(e) Monitoring for suspicious or unknown users;

(f) Monitoring for suspicious or irregular server requests;

(g) Monitoring for server requests for Personal Information;

(h) Monitoring for server requests for VPNs; and

(i) Monitoring for server requests from Tor exit nodes.

119. Here, 23andMe failed to take the proper steps to detect and prevent the unauthorized access. Credential stuffing generally has a very low rate of success at around 0.1% -- meaning a threat actor will succeed only once for every thousand attempts to use a recycled password from a large list.[21] The fact that 23andMe admits roughly 14,000 accounts were successfully accessed means the threat actor likely made around ***14 million failed login attempts***. If 23andMe had even basic threat detection tools in place, it would have detected such a large pattern of suspicious activity in real time and had ample opportunity to shut it down. Similarly, the automated process by a threat actor to access 5-7 million DNA Relatives profiles was an anomalous pattern of access that should have been detected by Defendant's threat detection protocols.

120. Had 23andMe implemented adequate monitoring systems in line with industry guidance, it could have detected these patterns of activity at the onset of the compromise and taken steps to prevent further malicious logins as well the further access to and eventual exfiltration of its customers' highly sensitive genetic data.

121. 23andMe also failed to adequately anticipate and prevent reasonably foreseeable hacking threats. Credential-stuffing attacks are a common security threat that have garnered a significant amount of attention due to breaches at other large companies by hackers using recycled user passwords. For this type of attack, hackers often buy credentials from these previous breaches, knowing that users often reuse passwords. 23andMe was well aware of the threat of this type of attack and even posted warnings in its privacy policies writing, "[b]e mindful of keeping your

[21] CloudFlare, *What is Credential Stuffing?* https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/#:~:text=Statistically%20speaking%2C%20credential%20stuffing%20attacks,they%20will%20succeed%20roughly%20once (last visited Apr. 16, 2024).

password and other authentication information safe from third parties, and immediately notify 23andMe of any unauthorized use of your login credentials." Despite this knowledge, 23andMe apparently placed the burden on users of the platform to report unusual activity, when it could have proactively protected customer information by requiring them to use multi-factor authentication for their accounts – a feature that had been optional on the platform since 2019.

122. In fact, 23andMe implicitly admitted that the breach could have been prevented with two-step verification. On November 6, 2023 – more than a month after the Breach Forum leak – 23andMe finally began requiring customers to use two-step verification because it "provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords." Many companies have had mandatory two-step verification in place for years. For example, Ring, a leading manufacturer of home security systems and cameras, added the requirement roughly four years ago. Had 23andMe implemented industry standard protections (or "exceed" them as promised), it would have required two-step verification prior to this breach.

123. Beyond two-step verification, the Open Source Foundation for Application Security ("OWASP"), a peer-reviewed industry resource, provides a number of basic, industry standard measures that 23andMe could have implemented to protect against a credential-stuffing attack including, implementing a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) for each login attempt, blocking known malicious or abusive IP addresses or devices, or even requiring users to create a username as opposed to an email address (which would have been listed in illicit information obtained by hackers to conduct a credential-stuffing attack).[22] Had 23andMe implemented ***any*** of these security processes, the credential-stuffing attack could have been thwarted entirely.

124. Before the Data Breach, 23andMe also failed to inform users of the increased risks of using the DNA Relatives feature. 23andMe knew or should have known through a risk assessment that the DNA Relatives function could compromise the integrity of numerous customer

[22] *Credential Stuffing Prevention Cheat Sheet*, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html (last visited Apr. 16, 2024).

profiles if a single associated account was breached. Nevertheless, there were no additional safeguards, protections, or warnings in place to alert users to increased threats when using this feature. If users had known of the potential for the widespread compromise of user accounts through this feature, they would have likely opted out.

125. The unauthorized acquisition of such a massive amount of user data during the Data Breach further showed that 23andMe failed to institute reasonable security measures to prevent or detect the attack including, monitoring for unusual login patterns and rates, utilizing up-to-date audit and traceability tools to monitor for suspicious activity, as well as threat detection and monitoring alerts that trigger when in real time data is exfiltrated at large volumes. Any of these basic security measures would have detected and mitigated the credential-stuffing attack and unauthorized data scraping of the DNA Relatives function.

126. While 23andMe publicly touted that it was certified in information security standards such as ISO/IEC 27001:2013, 27018, and 27701, it failed to upgrade its certifications to the newer 2022 versions, which contained pertinent policies that could have addressed the potential sources of the breach described here. For example, the new controls in updated versions include topics of threat intelligence, data leakage prevention, and monitoring activities, all of which are relevant to the Data Breach.[23]

127. 23andMe also knew or should have known about industry best practices aimed at preventing common data security threats, including a credential-stuffing attack. OWASP Top 10, a peer-reviewed industry standard document, highlighted the top web vulnerabilities against which companies should defend themselves.[24] Among these threats, the category "Identification and Authentication Failures" highlights security weakness that "permit automated attacks such as credential stuffing."[25] Another category, "Security Logging and Monitoring Features," outlines

[23] *ISO/IEC 27001& ISO/IEC 27002:2022: What You Need to Know*, PECB (Mar. 28, 2022) https://pecb.com/past-webinars/isoiec-27001--isoiec-270022022-what-you-need-to-know.

[24] *OWASP Top 10: 2021*, OWASP Top 10:2121, https://owasp.org/Top10/ (last visited Apr. 16, 2024).

[25] *A07:2021—Identification and Authentications Failures*, OWASP, https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ (last visited

best practices to "detect, escalate, and respond to active breaches" including appropriate alerting thresholds, monitoring logins and high-value transactions, and monitoring suspicious activities.[26]

H. 23andMe Failed to Comply with FTC Guidelines

128. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[27]

129. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems.

130. The FTC recommends that businesses:

(a) Identify all connections to the computers where you store sensitive personal information.

(b) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

(c) Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting his business.

Apr. 16, 2024).

[26] *A09:2021 — Security Logging and Monitoring Failures*, OWASP, https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ (last visited Apr. 16, 2024).

[27] Federal Trade Commission, *Start with Security: a Guide for Business, Lessons Learned from FTC Cases*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Apr. 16, 2024).

(d) Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

(e) Pay particular attention to the security of their web applications – the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

(f) Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

(g) Determine whether a border firewall should be installed where the business' network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls – settings that determine which devices and traffic get through the firewall – to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, he should be reviewed periodically.

(h) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

(i) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

131. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade

Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

132. Because Plaintiffs and Class members entrusted Defendant with their Personal Information, Defendant had, and still has, a duty to Plaintiffs and Class members to keep their Personal Information secure.

133. Plaintiffs and Class members reasonably expected that when they provided their Personal Information to 23andMe, it would safeguard their Personal Information.

134. 23andMe was at all times fully aware of its obligation to protect the personal and financial data, including that of Plaintiffs and Class members. 23andMe was also aware of the significant repercussions if it failed to do so.

135. 23andMe's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data – including Plaintiffs' and Class members' first, middle, and last names, addresses, and genetic information and ancestry – constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

I. The Data Breach Caused Concrete Injuries to Plaintiffs and the Class

136. Plaintiffs and Class members reasonably expected that 23andMe would provide adequate security protections for their Personal Information, and Plaintiffs and Class members provided Defendant with sensitive personal information as a result.

137. Defendant's poor data security deprived Plaintiffs and Class members of the benefit of their bargain and now has put them in danger. Plaintiffs and Class members understood and expected that, as part of that relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class members received data security services that were of a lesser value than what they reasonably expected. As such, Plaintiffs and Class members suffered pecuniary injury.

138. Cybercriminals intentionally attack and exfiltrate Personal Information to exploit it. Thus, Plaintiffs and Class members are now, and for the rest of their lives will be, at a heightened and substantial risk of hate crimes and other issues, as a consequence of the Data Breach. Plaintiffs and Class members have also incurred (and will continue to incur) damages in the form of, *inter*

alia, loss of privacy and costs of engaging adequate monitoring and identity theft protection services.

139. The hackers are already selling Plaintiffs' and Class members' information on the dark web, which not only jeopardizes Plaintiffs and Class members and could subject them to hate crimes and violence, but also to other issues including identity fraud, problems with insurance companies and obtaining insurance, and problems with obtaining employment.

140. Given Defendant's failure to timely provide notice, moreover, Plaintiffs and Class members were prevented from taking actions to protect themselves from these harms, such as the harm of being identified as Jewish.

141. Accordingly, as a direct and/or proximate result of 23andMe's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of hate crimes, identity theft and identity fraud. Even data that has not yet been exploited by cybercriminals bears a high risk that the hackers, who now possess Plaintiffs' and Class Members' Personal Information and are presently attempting to sell it on the dark web, will exploit the data at a later date or re-sell it to other possible bad actors.

142. As a result, Plaintiffs and Class members have already suffered damages, including an imminent risk that they could be subject to hate crimes and violence.

CLASS ACTION ALLEGATIONS

143. Plaintiffs bring this case as a class action pursuant to Rule 23(b)(1), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on their own behalf and as the Class representative on behalf of the following:

> **National Class:** All 23andMe customers residing within the United States whose Personal Information was compromised in the Data Breach.
>
> **Chinese and Ashkenazi Subclass:** All 23andMe customers of Chinese or Ashkenazi Jewish descent residing within the United States whose Personal Information was compromised in the Data Breach.

144. Plaintiff Roe also brings this case on behalf of the following:

Florida Class: All 23andMe customers residing in Florida whose Personal Information was compromised in the Data Breach.

Florida Chinese and Ashkenazi Subclass: All 23andMe customers of Chinese or Ashkenazi Jewish descent residing in Florida whose Personal Information was compromised in the Data Breach.

145. Plaintiff Public also brings this case on behalf of the following:

New Jersey Class: All 23andMe customers residing in New Jersey whose Personal Information was compromised in the Data Breach.

New Jersey Chinese and Ashkenazi Subclass: All 23andMe customers of Chinese or Ashkenazi Jewish descent residing in New Jersey whose Personal Information was compromised in the Data Breach.

146. Collectively, the National Class, the Florida Class, and the New Jersey Class are referred to as the "Class" or the "Classes."

147. Plaintiffs reserve the right to amend the Class definitions if further investigation and discovery indicate that the Class definitions should be narrowed, expanded, or otherwise modified.

148. Excluded from the Class are Defendant's officers, directors, agents, legal representatives, and employees.

149. This action has been brought and may be maintained as a class action under the Federal Rules of Civil Procedure.

A. Numerosity

150. Federal Rule of Civil Procedure 23(a)(1). This Class numbers over one million persons. As a result, joinder of all Class members in a single action is impracticable. Class members may be informed of the pendency of this class action through a variety of means, including, but not limited to, direct mail, email, published notice, and website posting.

B. Existence and Predominance of Common Questions of Law and Fact

151. Federal Rule of Civil Procedure 23(a)(2) and (b)(3). There are questions of fact and law common to the Classes that predominate over any question affecting only individual members.

Those questions, each of which may also be certified under Rule 23(c)(4), include, but are not limited to:

(a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Personal Information;

(b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(c) Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

(d) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

(e) Whether Defendant owed a duty to Plaintiffs and Class members to safeguard their Personal Information;

(f) Whether Defendant breached its duty to Plaintiffs and Class members to safeguard their Personal Information;

(g) Whether unauthorized third parties obtained Plaintiffs' and Class members' Personal Information in the Data Breach;

(h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

(i) Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendant's misconduct including an increase in imminent danger;

(j) Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

(k) Whether Defendant failed to provide an adequate data breach notice; and

(l) Whether Plaintiffs and Class members are entitled to damages and/or equitable relief.

C. Typicality

152. Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of those of the Class because Plaintiffs' Personal Information, like that of every other Class member, was compromised in the Data Breach and all Class members are subject to the same risk of imminent danger as a result of the Data Breach.

D. Superiority

153. Federal Rule of Civil Procedure 23(b)(3). A class action is the appropriate method for the fair and efficient adjudication of this controversy. The presentation of separate actions by individual Class members could create a risk of inconsistent adjudications, establish incompatible standards of conduct for Defendant, and/or substantially impair or impede the ability of Class members to protect their interests. In addition, it would be impracticable and undesirable for each member of the Class who suffered an economic loss to bring a separate action. The maintenance of separate actions would place a substantial and unnecessary burden on the courts and could result in inconsistent adjudications, while a single class action can determine, with judicial economy, the rights of all Class members.

E. Adequacy

154. Federal Rule of Civil Procedure 23(a)(4). Plaintiffs are adequate representatives of the Class because they are members of the Class and their interests do not conflict with the interests of the Class that they seek to represent. The interests of the members of the Class will be fairly and adequately protected by Plaintiffs and their undersigned counsel.

F. Declaratory and Injunctive Relief

155. Federal Rule of Civil Procedure 23(b)(2). Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to Class members as a whole.

156. Additionally, the Class may be certified under Rule 23(b)(1) and/or (b)(2) because:

(a) The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct for Defendant;

(b) The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class members who are not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to Class members as a whole.

CAUSES OF ACTION

COUNT I

Violation of California's Unfair Competition Law ("UCL") – Unlawful and Unfair Business Practices (Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On behalf of Plaintiffs and the National Class)

157. Plaintiffs reallege and incorporate by reference paragraphs 1 through 156 above as if fully set forth herein.

158. As discussed above, 23andMe's acts, practices, and omissions at issue in this matter, particularly those related to data security, were directed and emanated from its headquarters in Sunnyvale, California. Moreover, under Defendant's Terms of Use, California law applies to all Class members.

159. As customers, Plaintiffs and Class members entrusted 23andMe with their Personal Information.

160. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

161. Defendant stored Plaintiffs' and Class members' Personal Information in its electronic information databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal

regulations and that would have kept Plaintiffs' and Class members' Personal Information secure and prevented the loss or misuse of Plaintiffs' and Class members' Personal Information. 23andMe did not disclose to Plaintiffs and Class members that its data systems were not secure and misrepresented just the opposite, that, in fact, such information was secure and that customers' privacy and security were of paramount importance.

162. Plaintiffs and Class members relied upon Defendant's misrepresentations and were entitled to assume, and did assume, Defendant would take appropriate measures to keep their Personal Information safe when they complied with commercial protocols and divulged their Personal Information to Defendant, consistent with Defendant's representations. Defendant did not disclose at any time that Plaintiffs' and Class members' Personal Information was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

163. Defendant violated the UCL by misrepresenting, both by affirmative conduct, affirmative misrepresentations and by omission, the safety of its many systems and services, specifically the security thereof, and his ability to safely store Plaintiffs' and Class members' Personal Information.

164. Defendant also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and Class members of the Data Breach and to provide adequate notice. If Defendant had complied with these legal requirements, Plaintiffs and Class members would not have suffered the damages related to the Data Breach.

165. Further, as alleged here in this Complaint, 23andMe engaged in unlawful and unfair business practices in the conduct of business transactions, in violation of the UCL, by and including its:

(a) failure to maintain adequate computer systems and data security practices to safeguard Personal Information;

(b) failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information from theft;

(c) failure to timely and accurately disclose the Data Breach to Plaintiffs and Class members; and

(d) making misrepresentations about the safety of its website and Plaintiffs' and Class members' Personal Information.

166. 23andMe knew or should have known that its data security practices were inadequate to safeguard the Plaintiffs' and Class members' Personal Information, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

167. As a direct and proximate result of 23andMe's violation of the UCL, Plaintiffs and Class members have suffered damages, and are susceptible to damages, including an increased risk of hate crimes, danger and violence from anti-Semitic groups, and from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

168. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to consumers about Defendant's data security cannot be said to have had any utility at all. Thus, for example, there was no utility in using inadequate data security systems and protocols. Likewise, there was no utility in Defendant telling the Class that it used "physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information," and that it "regularly reviews and improves security practices to help ensure the integrity of our systems and your Personal Information," when neither was true. And, there was no utility, other than perhaps to Defendant itself, in unreasonably waiting to disclose the Data Breach. All of these actions and omissions were clearly injurious to Plaintiffs and Class members, directly causing the harms alleged below.

169. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described in detail above, violated fundamental public

policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them. . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a)(1) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions, and the injuries caused by them are thus comparable to or the same as a violation of the law.

170. Plaintiffs and Class members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. In addition, their Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Further, Plaintiffs and Class members have lost the benefit of their bargain and purchased services they otherwise would not have, or paid more for supposedly secure services than they would have, had they known the truth regarding Defendant's inadequate data security.

171. As a result of Defendant's unlawful and unfair business practices and violations of the UCL, Plaintiffs and the members of the Class are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

COUNT II

NEGLIGENCE
(On behalf of Plaintiffs and the National Class)

172. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 156 above as if fully set forth herein.

173. As part of the regular course of its business operations, Defendant gathered and stored Plaintiffs' and Class members' Personal Information.

174. Plaintiffs and the Class were entirely dependent on Defendant to use reasonable measures to safeguard their Personal Information and were vulnerable to the foreseeable harm of a security breach should Defendant fail to safeguard their Personal Information.

175. By collecting and storing this data in its computer property, sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property – and Class members' Personal Information held within it – to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

176. Defendant owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

177. Defendant's duty also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as 23andMe. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

178. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

179. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of his failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class members.

180. Defendant gathered and stored Plaintiffs' and Class members' Personal Information as part of its business of soliciting its services to its clients, which solicitations and services affect commerce.

181. Defendant violated the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class members' Personal Information and by not complying with applicable industry standards.

182. Defendant breached its duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard their Personal Information, and by failing to provide prompt notice without reasonable delay.

183. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who sought to use its services, which is recognized by laws and regulations, including, but not limited to, the FTC Act, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class members, or minimize the Data Breach.

184. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Personal Information.

185. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiffs could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

186. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and Class members had no ability to protect their Personal Information that was in Defendant's possession.

187. Defendant was in a special relationship with Plaintiffs and Class members with respect to the stolen Personal Information because the aim of Defendant's data security measures was to benefit Plaintiffs by ensuring that their Personal Information would remain protected and secure. Only Defendant was able to ensure that its systems were sufficiently secure to protect

Plaintiffs' and Class members' Personal Information. The harm to Plaintiffs and the Class from its exposure was highly foreseeable to Defendant.

188. Defendant owed Plaintiffs and Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and Class members when obtaining, storing, using, and managing their Personal Information, including acting to reasonably safeguard such data and providing notification to Plaintiffs and the Class of any breach in a timely manner so that appropriate action could be taken to minimize losses.

189. Defendant had duties to protect and safeguard the Personal Information of Plaintiffs and Class members from being vulnerable to compromise by taking common-sense precautions when dealing with highly sensitive Personal Information. Additional duties that Defendant owed Plaintiffs and the Class include:

(a) Exercising reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures, and practices to ensure that Personal Information was adequately secured from impermissible release, disclosure, and publication;

(b) Protecting Plaintiffs' and Class Members' Personal Information in its possession by using reasonable and adequate security procedures and systems; and

(c) Promptly notifying Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Personal Information.

190. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that had been entrusted to them.

191. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and the Class' Personal Information. Defendant breached its duties by failing to:

(a) Exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Personal Information in its possession;

(b) Protect the Personal Information in its possession using reasonable and adequate security procedures and systems;

(c) Adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal Information;

(d) Consistently enforce security policies aimed at protecting Plaintiffs' and the Class' Personal Information;

(e) Mitigate the harm caused to Plaintiffs and the Class;

(f) Implement processes to quickly detect data breaches, security incidents, or intrusions; and

(g) Promptly notify Plaintiffs and Class members of the Data Breach.

192. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

193. 23andMe, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' during the time the Personal Information was within Defendant's possession or control.

194. Defendant's failure to provide timely and clear notification of the Data Breach to Plaintiffs and the Class prevented them from taking meaningful, proactive steps to securing their Personal Information and mitigating damages.

195. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

196. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including, but not limited to: (a) danger of hate crimes and violence, (b) the loss of the opportunity to choose how their Personal Information is used; (c) the compromise, publication, and/or theft of their Personal Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from hate crimes and unauthorized use of their Personal Information; (e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (f) the continued risk to their Personal Information,

which remain in Defendant's possession, and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in his continued possession; (g) the loss of their benefit of their bargain for Defendant's services; and (h) future costs.

197. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered (and will continue to suffer) other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

198. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class members suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's possession, and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

199. Plaintiffs and Class members have suffered injury and are entitled to actual damages in amounts to be proven at trial.

COUNT III

Breach of Implied Contract
(On behalf of Plaintiffs and the National Class)

200. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 156 above as if fully set forth herein.

201. Plaintiffs and Class members were required to provide their Personal Information to Defendant as a condition of receiving services provided by Defendant.

202. Plaintiffs and Class members provided Personal Information to Defendant in exchange for services. In exchange, Defendant promised to protect their Personal Information from unauthorized disclosure.

203. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiffs and Class members that it would only

disclose Personal Information under certain circumstances, none of which relate to the Data Breach.

204. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class members' Personal Information would remain protected.

205. Implicit in the agreement between Plaintiffs, Class members, and Defendant to provide Personal Information, was the latter's obligation to: (a) use such Personal Information for business purposes only; (b) take reasonable steps to safeguard that Personal Information; (c) prevent unauthorized disclosures of the Personal Information; (d) provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Personal Information; (e) reasonably safeguard and Plaintiffs and Class members' Personal Information from unauthorized disclosure or use; and (f) retain the Personal Information only under conditions that kept such information secure and confidential.

206. Defendant required Plaintiffs' and Class members to provide their Personal Information as part of its regular business practices.

207. When Plaintiffs and Class members provided their Personal Information to Defendant as a condition of the consumer relationship, implied contracts were created with Defendant. As such, Defendant agreed to reasonably protect such information.

208. Plaintiffs and Class members entered into the implied contracts with the reasonable expectation and belief that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

209. Plaintiffs and Class members believed that 23andMe would use part of the monies paid to Defendant under the implied contracts or the monies obtained from the benefits derived from the Personal Information they provided to fund adequate and reasonable data security practices.

210. Plaintiffs and Class members would not have entrusted their Personal Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class members would not have entrusted their

Personal Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures. The safeguarding of Plaintiffs' and Class members' Personal Information was critical to realize the intent of the parties.

211. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

212. Defendant breached its implied contracts with Plaintiffs and Class members by failing to safeguard and protect their Personal Information.

213. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class members sustained damages.

214. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

215. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate long term threat monitoring and protection to Plaintiffs and Class members.

COUNT IV

Unjust Enrichment
(On behalf of Plaintiffs and the National Class)

216. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 156 above as if fully set forth herein.

217. Plaintiffs and Class members conferred a monetary benefit upon Defendant in the form of purchasing products from Defendant, and in connection thereto, by providing their Personal Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their Personal Information. In

exchange, Plaintiffs and Class members should have received adequate protection and data security for such Personal Information held by Defendant.

218. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Personal Information of Plaintiffs and Class members for business purposes.

219. Acceptance of the benefit under these facts and circumstances make it inequitable for Defendant to retain that benefit without payment of the value thereof. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Personal Information. This is evidenced by Defendant's mentions of multifactor authentication and its terms of service and eventual adoption of the same on November 6, 2023.

220. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members thus suffered as a direct and proximate result of Defendant's decision to prioritize profits over the requisite data security.

221. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class members because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

222. Defendant acquired the Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

223. If Plaintiffs and Class members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

224. Plaintiffs and Class members have no adequate remedy at law.

225. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

226. For the benefit of Plaintiffs and Class members, Defendant should be compelled to disgorge proceeds that it unjustly received from them into a common fund or constructive trust.

COUNT V

Invasion of Privacy
(On behalf of Plaintiffs and the National Class)

227. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 156 above as if fully set forth herein.

228. Plaintiffs and Class members had a legitimate expectation of privacy in their Personal Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

229. Defendant owed a duty to Plaintiffs and Class members, to keep their Personal Information confidential.

230. Defendant failed to protect, and allowed unknown and unauthorized third parties to access, the Personal Information of Plaintiffs and Class members.

231. The Personal Information that was publicized during the Data Breach was highly sensitive, private, and confidential.

232. Defendant acted with reckless disregard for the privacy of Plaintiffs and Class members rising to the level of: (a) an intentional intrusion by Defendant; (b) into a matter that Plaintiffs and Class members have a right to keep private (*i.e.*, their Personal Information); and (c) which is highly offensive to a reasonable person.

233. Defendant acted knowingly when it permitted the Data Breach to occur; it had actual knowledge that its information security practices were inadequate and insufficient.

234. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class members' data and Personal Information.

235. Defendant acted with such reckless disregard as to the safety of Plaintiffs' and Class members' Personal Information to rise to the level of intentionally allowing the intrusion upon Plaintiffs' and Class members' seclusion.

236. The unauthorized release to, custody of, and examination by unauthorized third parties of the Personal Information of Plaintiffs and Class members is highly offensive to a reasonable person.

237. Plaintiffs and Class members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT VI

Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.*
(On Behalf of Plaintiff Roe and the Florida Class)

238. Plaintiff Roe repeats the allegations contained in paragraphs 1 through 156 as if fully set forth herein.

239. Plaintiff Roe brings this claim on behalf of himself and the Florida Class.

240. This cause of action is brought under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

241. 23andMe offers, provisions, and sales or services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-213.

242. Plaintiff Roe and Florida Class Members are "individual[s]," and are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

243. 23andMe offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

244. Plaintiff Roe and Florida Class Members paid for or otherwise availed themselves and received services from 23andMe, primarily for personal, family, or household purposes.

245. 23andMe engaged in the conduct alleged herein, entering into transactions intended to result, and which did result, in the provision of genetic testing and genealogical research services to or for Plaintiff Roe and Florida Class Members.

246. 23andMe's acts, practices, and omissions were done in the course of 23andMe's business of offering and selling genetic testing and geological research services throughout Florida and the United States.

247. The unfair, unconscionable, and unlawful acts and practices of 23andMe alleged herein, and in particular the decisions regarding data security, emanated and arose – with respect to Florida Class Members, within the state of Florida, within the scope of the FDUTPA.

248. 23andMe, operating in Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

(a) failing to implement and maintain reasonable and adequate computer systems and data security practices to safeguard customer Personal Information;

(b) omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard customer Personal Information from unauthorized access and theft;

(c) failing to protect the privacy and confidentiality of Plaintiff Roe's and Florida Class Members' Personal Information; and

(d) failing to disclose that the hackers had targeted and posted Personal Information of customers of Chinese and Ashkenazi Jewish descent.

249. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 45, and the FDUTPA, Fla. Stat. § 501.171(2).

250. 23andMe knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff Roe and Florida Class Members' Personal Information and that the risk of a data breach or theft was high.

251. Plaintiff Roe has standing to pursue this claim because as a direct and proximate result of 23andMe's violations of the FDUTPA, Plaintiff Roe and Florida Class Members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that 23andMe's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

252. Plaintiff Roe also has standing to pursue this claim because, as a direct result of 23andMe's knowing violation of the FDUTPA, Plaintiff Roe and the Florida Class are at a substantial and imminent risk of harm as a result of the Data Breach. 23andMe still possesses Plaintiff Roe's and the Florida Class Members' Personal Information, and that Personal Information has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of harm to Plaintiff Roe and all Florida Class members, as well as a risk of theft of their Personal Information.

253. Plaintiff Roe and Florida Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of identity theft, including, but not limited to:

(a) ordering that 23andMe engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

(b) ordering that 23andMe engage third-party security auditors and internal personnel to run automated security monitoring;

(c) ordering that 23andMe audit, test, and train security personnel regarding any new or modified procedures;

(d) ordering that 23andMe segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

(e) ordering that 23andMe purge, delete, and destroy customer Personal Information not necessary for its provisions of services in a reasonably secure manner;

(f) ordering that 23andMe conduct regular database scans and security checks;

(g) ordering that 23andMe routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(h) ordering 23andMe to meaningfully educate customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the

steps present and former customers should take to protect themselves; and

(i) ordering 23andMe to take reasonable steps to protect Plaintiff Roe and Florida Class members against harm from misuse of their Personal Information that was misappropriated in the Data Breach.

254. Plaintiff Roe brings this action on behalf of himself and Florida Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff Roe, Florida Class Members, and the public from 23andMe's unfair methods of competition and unfair, unconscionable, and unlawful practices. 23andMe's wrongful conduct as alleged in herein has had widespread impact on the public at large.

255. The above unfair, unconscionable, and unlawful practices and acts by 23andMe were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Roe and Florida Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

256. 23andMe's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices and described herein were negligent, knowing and willful, and/or wanton and reckless.

257. Plaintiff Roe and Florida Class Members seek relief under the FDUTPA, Fla. Stat. § 501.201, *et seq.*, including, but not limited to: damages; restitution; a declaratory judgment that 23andMe's actions and/or practices violate the FDUTPA; injunctive relief enjoining 23andMe, their employees, parents, subsidiaries, affiliates, executives, and agents from violating the FDUTPA; an order that 23andMe engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors; an order that 23andMe engage third-party security auditors and internal personnel to run automated security monitoring; an order that 23andMe audit, test, and train security personnel regarding any new or modified procedures; an order that 23andMe segment customer data by, among other things, creating firewalls and access controls so that if one

area of a network system is compromised, hackers cannot gain access to other portions of the system; ordering that 23andMe conduct regular database scans and security checks; an order that 23andMe routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; an order requiring 23andMe to meaningfully educate customers about the threats they face as a result of the loss of their personal information to third parties, as well as the steps current and former customers should take to protect themselves; an order requiring 23andMe to take reasonable steps to protect Plaintiff Roe and Florida Class members against harm from misuse of their Personal Information that was misappropriated in the Data Breach; attorneys' fees and costs; and any other just and proper relief.

COUNT VI

New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. § 56:8-2
(On Behalf of Plaintiff Public and the New Jersey Class)

258. Plaintiff Public re-alleges and incorporates by reference paragraphs 1 through 157 as if fully set forth herein.

259. Plaintiff Public brings this claim on behalf of himself and the New Jersey Class.

260. The New Jersey CFA makes unlawful "[t]he act, use or employment by any person of any ***unconscionable commercial practice***, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J.S.A. § 56:8-2 (emphasis added).

261. 23andMe, Plaintiff Public, and Class members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

262. 23andMe engaged in "sales" of "merchandise" within the meaning of N.J.S.A. § 56-8-1(c), (d).

263. Plaintiff Public and Class members are consumers who made payments to 23andMe for the furnishing of services that were primarily for personal, family, or household purposes.

264. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. The standard of conduct the term "unconscionable" entails is a lack of good faith, honesty in fact, and observance of fair dealing. Intent is not an element for allegations related to unconscionable commercial practices.

265. Here, 23andMe's conduct was unconscionable under the New Jersey CFA in its failure to maintain adequate data security and to safeguard the PII in its possession.

266. Specifically, 23andMe's handling and protection of Plaintiff Public's and Class members' PII was unconscionable commercial practice for the following reasons, among others.

267. Plaintiff Public and Class members had no choice as to whether to provide their PII to 23andMe, nor the categories of PII, in order to use 23andMe's services.

268. The terms and conditions under which Plaintiff Public and Class members agreed to provide PII to 23andMe, and how 23andMe was to protect their PII were non-negotiable and were presented on a take-it-or-leave it basis to Plaintiff Public and Class members.

269. Plaintiff Public and Class members were unable to discover the true state of 23andMe's data security measures and take measures on their own to protect their PII once it was in 23andMe's possession. Thus, Plaintiff Public and Class members were completely dependent upon 23andMe to protect their PII once it was in 23andMe's possession.

270. Indeed, 23andMe lulled Plaintiff Public and Class members into a false sense of security by representing that their PII would be well-taken-care-of. 23andMe specifically states in its Privacy Statement that:

> When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected.

271. With respect to protection of PII in general, 23andMe stated that:

> 23andMe takes seriously the trust you place in us. To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of information, 23andMe uses a range of physical, technical, and administrative measures to safeguard your Personal Information, in accordance with current

> technological and industry standards. In particular, all connections to and from our website are encrypted using Secure Socket Lays (SSL) technology.

272. 23andMe, operating in New Jersey, engaged in unconscionable trade acts or practices in the conduct of trade or commerce, in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

(a) failing to implement and maintain reasonable and adequate computer systems and data security practices to safeguard customer PII;

(b) omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard customer PII from unauthorized access and theft;

(c) failing to protect the privacy and confidentiality of Plaintiff Public's and New Jersey Class Members' PII; and

(d) failing to disclose that the hackers had targeted and posted Personal Information of customers of Chinese and Ashkenazi Jewish descent.

273. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 45, and the New Jersey CFA, N.J.S.A. § 56:8-163.

274. 23andMe's data protection practices are contrary to public policy in that they fail to comply with FTC rules and regulations relating to data security and other applicable standards as is set forth above.

275. 23andMe still possesses Plaintiff Public's and Class members' PII, and that PII has been both accessed and misused by unauthorized third parties. Plaintiff Public and Class members will have to spend the remainder of their lives at greater risk for harm, identity theft, and fraud (having to constantly monitor for the same).

276. The foregoing unconscionable commercial practices emanated from New Jersey and were directed at consumers/purchasers in New Jersey and in each state where Defendant did business.

277. As a direct and proximate result of 23andMe's multiple, separate violations of N.J.S.A. § 56:8-2, Plaintiff Public and Class members suffered ascertainable losses including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in 23andMe's possession and is subject to further unauthorized disclosures so long as 23andMe fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff Public and Class members; and (g) the diminished value of 23andMe's services they received.

278. Plaintiff Public and New Jersey Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of identity theft, including, but not limited to:

(a) ordering that 23andMe engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

(b) ordering that 23andMe engage third-party security auditors and internal personnel to run automated security monitoring;

(c) ordering that 23andMe audit, test, and train security personnel regarding any new or modified procedures;

(d) ordering that 23andMe segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

(e) ordering that 23andMe purge, delete, and destroy customer PII not necessary for its provisions of services in a reasonably secure manner;

(f) ordering that 23andMe conduct regular database scans and security checks;

(g) ordering that 23andMe routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(h) ordering 23andMe to meaningfully educate customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps present and former customers should take to protect themselves; and

(i) ordering 23andMe to take reasonable steps to protect Plaintiff Public and New Jersey Class members against harm from misuse of their PII that was misappropriated in the Data Breach.

279. Plaintiff Public and Class members were injured because they: (a) they would not have paid for Defendant's services had they known the true nature and character of 23andMe's data security practices; (b) would not have entrusted their PII to 23andMe in the absence of promises that Defendant would keep their information reasonably secure; and/or (c) would not have entrusted their PII to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

280. On behalf of himself and other members of the Class, Plaintiff Public is entitled to recover legal and/or equitable relief, including an order enjoining 23andMe's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J.S.A. § 56:8-19, and any other just and appropriate relief.

COUNT VII

Declaratory Judgment
(On behalf of Plaintiffs and the National Class)

281. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 157 above as if fully set forth herein.

282. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

283. An actual controversy has arisen in the wake of Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Personal Information.

284. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs and Class members will continue to suffer injury as a result of the compromise of their Personal Information, and remain at imminent risk that further compromises their Personal Information will occur in the future.

285. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) 23andMe continues to owe a legal duty to secure its users' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

(b) 23andMe continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class members' Personal Information.

286. The Court also should issue corresponding prospective injunctive relief requiring that 23andMe employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

287. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at 23andMe occurs, Plaintiffs and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

288. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to 23andMe if an injunction is issued. Among other things, if another massive data breach occurs at 23andMe, Plaintiffs and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to 23andMe of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and 23andMe has a preexisting legal obligation to employ such measures.

289. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at 23andMe, thus eliminating the additional injuries that would result to Plaintiffs and the millions of individuals whose Personal Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court enter judgment in his favor and against Defendant as follows:

A. For an Order certifying the Class under Federal Rule of Civil Procedure 23 and naming Plaintiffs as the representatives for the Class and Plaintiffs' attorneys as Class Counsel;

B. For an Order declaring Defendant's conduct violates the causes of action referenced herein;

C. For an Order finding in favor of Plaintiffs and the Class on all counts asserted herein;

D. Ordering Defendant to take all steps to obtain Plaintiffs' and Class members' Personal Information currently on the dark web and to take all steps to prevent the hackers from continuing to offer Plaintiffs' and other Class members' Personal Information on the dark web;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an Order of restitution and all other forms of equitable monetary relief;

H. For injunctive relief as pleaded or as the Court may deem proper;

I. For an Order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other and further relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs and Class members demand a trial by jury of any and all claims in this Complaint and of any and all issues in this action so triable as of right.

DATED: April 18, 2024

Respectfully submitted,

/s/ *Melissa A. Gardner*

Melissa A. Gardner (SBN 289096)
mgardner@lchb.com
Elizabeth J. Cabraser (SBN 83151)
ecabraser@lchb.com
Michael W. Sobol (SBN 194857)
msobol@lchb.com
Jallé Dafa (SBN 290637)
LIEFF CABRASER HEIMANN & BERNSTEIN LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000

Sean A. Petterson (*pro hac vice* forthcoming)
spetterson@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN LLP
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212.355.9500

ROBBINS GELLER RUDMAN & DOWD LLP
Dorothy P. Antullis (*pro hac vice* forthcoming)
Stuart A. Davidson (*pro hac vice* forthcoming)
Lindsey H. Taylor(*pro hac vice* forthcoming)
Alexander C. Cohen (*pro hac vice* forthcoming)
225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561.750.3000
dantullis@rgrdlaw.com
sdavidson@rgrdlaw.com
ltaylor@rgrdlaw.com
acohen@rdrglaw.com

ROBBINS GELLER RUDMAN & DOWD LLP
Aelish M. Baig (SBN 201279)
Taeva Shefler (SBN 291637)
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415.288.4545
aelishb@rgrdlaw.com
tshefler@rgrdlaw.com

Attorneys for Plaintiffs Richard Roe, John Q. Public, and the Proposed Class